IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

| | | | |
|---|---|---|---|
| Appellant: | Raikar et al. | Patent Application | |
| Serial No.: | 10/723,119 | Group Art Unit: | 2436 |
| Filed: | 11/25/2003 | Examiner: | Hoffman, Brandon |

For: METHOD AND SYSTEM FOR ESTABLISHING A CONSISTENT PASSWORD POLICY

Appeal Brief

Table of Contents

Real Party in Interest

The assignee of the present invention is Hewlett-Packard Company.

Related Appeals and Interferences

There are no related appeals or interferences known to the Appellant.

Status of Claims

Claims 1-22 are pending. Claims 1-22 stand rejected. Rejections of Claims 1-22 are herein appealed. Claims 23-24 are cancelled.

Status of Amendments

All proposed amendments have been entered. An amendment subsequent to the Final Action has not been filed.

Summary of Claimed Subject Matter

Independent Claim 1 recites a computer implemented method (method 200 of Figure 2 and page 14, second full paragraph) of establishing a consistent password policy. The method including describing (210 of Figure 2 and page 14, last paragraph) a plurality of password policies in a computer usable password policy data structure, accessing (220 of Figure 2 and page 18, second paragraph) the computer usable password policy data structure by a password policy enforcement agent, enforcing (240 of Figure 2 and page 18, last paragraph) at least one of the plurality of password policies described within the password policy data structure by the password policy enforcement agent, determining a strength of one of the plurality of password policies based on the enforcing and dynamically modifying (page 19, first paragraph) one of the plurality of password policies based on the strength.

Independent Claim 20 recites instructions on a computer usable storage medium wherein the instructions when executed cause a computer system to perform a method (method 200 of Figure 2 and page 14, second full paragraph) of establishing a consistent password policy, the method including describing (210 of Figure 2 and page 14, last paragraph) a plurality of password policies in a computer usable password policy data structure, providing an access point (tier 110 of Figure 1 and page ) with access to said computer usable password policy data structure, receiving (250 of Figure 2 and page 19, second paragraph) feedback from a password policy enforcement agent associated with said access point about which of said plurality of password policies have been successfully

enforced, determining (260 of Figure 2 and page 19, first paragraph) a strength of one of said plurality of password policies based on said feedback and dynamically modifying (page 19, first paragraph) one of said plurality of password policies based on said strength.

Grounds of Rejection to be Reviewed on Appeal

1. Claims 1-22 stand rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Arguments

**1. Whether Claims 1-22 are directed to statutory subject matter.**

Appellants have amended Claims 1-19 to be directed to a "computer implemented method" which is tied to a computer. A computer is a machine and thus Claims 1-19 satisfy requirement (1) set forth by the Examiner in section 5 of the current Action. As such, Appellants respectfully submit that Claims 1-19 are directed to statutory subject matter and Appellants respectfully request the rejection be removed.

Appellants have amended Claims 20-22 to be directed to a "computer usable storage medium" which is tied to a tangible article. As such, Appellants respectfully submit that Claims 20-22 are directed to statutory subject matter and Appellants respectfully request the rejection be removed.

Applicants respectfully disagree with the non-statutory statement. Applicants respectfully point out that MPEP 2106.01 clearly states

> When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized. Compare *In re Lowry*, 32 F.3d 1579, 1583-84, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994) (discussing patentable weight of data structure limitations in the context of a statutory claim to a data structure stored on a computer readable medium that increases computer efficiency) and *Warmerdam*, 33 F.3d at 1360-61, 31 USPQ2d at 1759 (claim to computer having a specific data structure stored in memory held statutory product-by-process

claim) with *Warmerdam*, 33 F.3d at 1361, 31 USPQ2d at 1760 (claim to a data structure *per se* held nonstatutory). (emphasis added)

Applicants respectfully submit that data disposed in a computer usable storage medium is indeed statutory as defined in the MPEP 2106.01. As such, Applicants respectfully submit that the rejection of Claims 20-22 under 35 U.S.C. §101 is incorrect and should be withdrawn.

In summary, the Appellant respectfully requests that the Board reverse the Examiner's rejections of claims 1-22.

The Appellant wishes to encourage the Examiner or a member of the Board of Patent Appeals to telephone the Appellant's undersigned representative if it is felt that a telephone conference could expedite prosecution.

Respectfully submitted,

WAGNER BLECHER LLP

Date: 04/26/2010

/John P. Wagner, Jr./

John P. Wagner, Jr.

Registration Number: 35,398

WAGNERBLECHER
WESTRIDGE BUSINESS PARK
123 WESTRIDGE DRIVE
WATSONVILLE, CALIFORNIA 95076
408-377-0550

Claims Appendix

1. A computer implemented method of establishing a consistent password policy, said method comprising:

describing a plurality of password policies in a computer usable password policy data structure;

accessing said computer usable password policy data structure by a password policy enforcement agent; ~~and~~

enforcing at least one of said plurality of password policies described within said password policy data structure by said password policy enforcement agent;

determining a strength of one of said plurality of password policies based on said enforcing; and

dynamically modifying one of said plurality of password policies based on said strength.

2. The computer implemented method of Claim 1 wherein said computer usable password policy data structure comprises a file structure compatible with extensible markup language.

3. The computer implemented method of Claim 1 wherein said password policy enforcement agent is operable on a client computer of a client-server computer system.

4. The computer implemented method of Claim 1 wherein said method is operable on a utility data center.

5. The computer implemented method of Claim 1 further comprising validating said computer usable password policy data structure for authenticity by said password policy enforcement agent.

6. The computer implemented method of Claim 1 wherein said plurality of password policies comprises a threshold parameter for unsuccessful access attempts that when exceeded disables a computer system access account.

7. The computer implemented method of Claim 6 wherein said plurality of password policies comprises a parameter indicating a time duration, and wherein exceeding said threshold parameter triggers locking of a computer system access account within said time duration.

8. The computer implemented method of Claim 1 wherein said plurality of password policies comprises an initial delay parameter to block access to a computer system access account for a period of time after an unsuccessful access attempt.

9. The computer implemented method of Claim 8 wherein access to said computer system access account is delayed for an increasing time period for successive unsuccessful access attempts.

10. The computer implemented method of Claim 1 wherein said plurality of password policies comprises a minimum password length parameter.

11. The computer implemented method of Claim 1 wherein said plurality of password policies comprises a maximum password length parameter.

12. The computer implemented method of Claim 1wherein said plurality of password policies comprises a parameter for prohibiting passwords comprising a word associated with a natural language.

13. The computer implemented method of Claim 12 wherein said natural language is English.

14. The computer implemented method of Claim 1 wherein said plurality of password policies comprises a parameter for prohibiting passwords comprising a palindrome.

15. The computer implemented method of Claim 1 wherein said plurality of password policies comprises a parameter for prohibiting passwords comprising a derivative of a computer system account name.

16. The computer implemented method of Claim 1 wherein said plurality of password policies comprises a parameter for automatically generating a password.

17. The computer implemented method of Claim 1 wherein said plurality of password policies comprises a parameter for automatically generating a pronounceable password consistent with said plurality of password policies.

18. The computer implemented method of Claim 1 wherein said plurality of password policies comprises a parameter for specifying a set of characters utilizable to automatically generate a password.

19. The computer implemented method of Claim 1 further comprising providing, by said password policy enforcement agent, feedback to a configuration and aggregation point, about whether said at least one of said plurality of password policies has been successfully enforced.

20. Instructions on a computer usable storage medium wherein the instructions when executed cause a computer system to perform a method of establishing a consistent password policy, said method comprising:

describing a plurality of password policies in a computer usable password policy data structure;

providing an access point with access to said computer usable password policy data structure;

receiving feedback from a password policy enforcement agent associated with said access point about which of said plurality of password policies have been successfully enforced;

determining a strength of one of said plurality of password policies based on said feedback; and

dynamically modifying one of said plurality of password policies based on said strength.

21. The computer usable storage medium of Claim 20 wherein said computer usable password policy data structure-comprises a file structure compatible with extensible markup language.

22. The computer usable storage medium of Claim 20 wherein said method further comprises:

selecting a computer access password policy parameter from said plurality of computer access password policy parameters consisting of a parameter selected from a group of parameters comprising a threshold parameter for unsuccessful access attempts that when exceeded disables a computer system access account, a parameter indicating the a time duration within which said threshold parameter number of unsuccessful access attempts triggers locking of a computer system access account, an initial delay parameter to block access to a computer system access account for a period of time after an unsuccessful

access attempt, a minimum password length parameter, a maximum password length parameter, a parameter to prohibit passwords consisting of a natural language word, a parameter to prohibit passwords consisting of a palindrome, a parameter to prohibit passwords consisting of a derivative of a computer system account name, a parameter to automatically generate a password, a parameter to automatically generate a pronounceable password consistent with all of said plurality of password policies, and a parameter to specify a set of characters utilizable to automatically generate a password.

Evidence Appendix

None

Related Proceedings Appendix

None